Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – October 2020

October is Cybersecurity Awareness Month

The annual campaign, led by the US Department of Homeland Security and the National Cyber Security Alliance (NCSA), is to educate and inform consumers, small and mid-sized businesses, corporations, educational institutions and young people about how to stay secure and safe while connected to the internet. The first observed NCSAM was October 2004. Now in its 17th year, National Cybersecurity Awareness Month (NCSAM) continues to raise awareness about the importance of cybersecurity across our nation, ensuring that all Americans have the resources they need to be safer and more secure online. CISA and the National Cyber Security Alliance (NCSA) are proud to announce this year's theme, ***"Do Your Part. #BeCyberSmart"***. This theme encourages individuals and organizations to own their role in protecting their part of cyberspace, stressing personal accountability and the importance of taking proactive steps to enhance cybersecurity. NCSAM emphasizes "If You Connect It, Protect It." Throughout October, CISA and NCSA will focus on the following areas in their promotions and outreach:

- October 1 and 2: Official NCSAM Kick-off
- Week of October 5: If You Connect It, Protect It
- Week of October 12: Securing Devices at Home and Work
- Week of October 19: Securing Internet-Connected Devices in Healthcare
- Week of October 26: The Future of Connected Devices

FinCEN Preparing to Modernize AML Guidelines

The US Financial Crimes Enforcement Network (**FinCEN**) has announced it will be changing the anti-money laundering (AML) and counter-terrorist financing (CTF) rules within the financial sector. In the announcement FinCEN will be seeking public feedback on regulatory proposals intended to modernize and strengthen rules governing the reporting and monitoring requirements of financial institutions. The new AML regulations focus on identifying and combating illicit financial activity through robust record-keeping and risk assessment requirements and FinCEN hopes to improve the definition and requirements of an effective and reasonably designed AML program.

SIRG's Asset Managers Council (AMC) Table Topic Exercise

On 24 September, the FS-ISAC's Securities Industry Risk Group (SIRG) Asset Manager Council ran its first ever tabletop exercise. The exercise focused on a trading firm's inability to trade due to a DDoS attack. The design of this tabletop was to help members who never experienced or participated in one to understand the process, as well as for other members who are novice in the practice as it focuses on each firm's core business. If you are interested to learn more about the exercise or the SIRG, please contact **sirg@fsisac.com** .

Staffing Shortage of Cybersecurity Professionals

Cybersecurity professionals are facing an obstacle that was prevalent prior to Covid19 arriving, a shortage of qualified workers. Prior to the pandemic, the need for cybersecurity workers was high. As employees started to work from home, many IT workers were pulled from projects being worked on to transition their workforces to a remote model. According to **(ICS)2**, at the end of 2019 there was an estimated 2.8 million cybersecurity professionals globally. That number falls short of the roughly 4 million needed to protect organizations.

AgentTesla Trojan Spreads via Covid-19 Phishing Scheme

Researchers from Area 1 Security have discovered **a global phishing campaign** that infects victims' devices with the **AgentTesla remote access Trojan** by claiming to offer information about surgical masks and other personal protective equipment (PPE) for using during the COVID-19 pandemic. The campaign, which is believed to have started in May 2020, uses phishing emails that look like they came from chemical manufactures, preying on fears of shortages of PPE during the pandemic.

The report states the fraudsters are making changes to their tactics and the messages every 10 days or so, to avoid detection. The phishing emails appear to have targeted thousands of people and contains an attachment that is disguised to look like a PDF file that is typically named: "Supplier-Face Mask Forehead Thermometer.pdf.gz". The goal of these emails is to infect devices with AgentTesla, a one-time information stealer that has been revamped as a remote access Trojan, or RAT. These RATs are effective because they have the ability to avoid detection as well as their low licensing feeds on unground forums that make it affordable to rent and deploy. Firms are advised to review the researcher report, educate end user of these phishing emails, and update all anti-virus and spam filters to help prevent these phishing emails from accessing their system.

Know Your Enemy

With its attractive business model and multiple revenue streams, ransomware is a growing threat to financial services and their third-party suppliers.

There are many steps you can take to prevent attacks, but threat actors are evolving their tactics all the time. If attacked, will you pay the ransom? Industry-specific threat intelligence is a critical tool in helping you decide.

With ransomware attacks growing globally, for Cyber Security Awareness Month we've released a **ransomware report** to help your financial institution prepare and combat ransomware.

CEOs to be Personally Liable for Cyber-Physical Security Incidents

The liability of cyber incidents, or cyber-physical systems (CPSs), may soon fall on roughly 75% of CEOs by 2024, according to a report from **Gartner**. By failing to secure CPSs, rules and regulations will increase dramatically. Some agencies in the US - FBI, NSA, and Cybersecurity and Infrastructure Security Agenda (CISA), have started to provide more information around threats to critical infrastructure-related systems. Given that more data is available to organizations, CEOs should no longer be caught off guard when incidents occurs. Moving forward, the key is to have technology leaders provide current and measurable updates to C-Suite executives.

This monthly update is brought to you by the Financial Services Information Sharing and Analysis Center (FS-ISAC) in coordination with the Investment Industry Association of Canada (IIAC), the International Council of Securities Associations (ICSA), the Financial Services Institute (FSI), the Insured Retirement Institute (IRI), the Securities Industry and Financial Markets Association (SIFMA) and the SPARK Institute.

The information provided in this monthly newsletter highlights cybersecurity topics and emerging threats to the securities industry globally. It is intended to increase the cybersecurity awareness of an organization's end-users and to help them interact in a more secure manner. This newsletter is not intended to replace the benefits of joining FS-ISAC. Learn more at fsisac.com.